Multi-Factor Authentication:
How MFA protects companies and their customers

Businesses have a problem. And it's growing. The number of records exposed from data breaches grew in the United States, from 198 million in 2017 to 446 million in 2018. According to Microsoft, phishing attacks rose by 250% in 2018. Ransomware attacks are on also the rise. So is cyber-espionage and traditional cyber crime. Here are just some recent attacks:

- **2018**—500 million records were stolen through unauthorized access of Marriott Starwood's guest database, including encrypted credit card information.
- **2018**—State Farm and Dunkin Donuts both fell victim to credential stuffing attacks, where hackers used combinations of leaked usernames and passwords, trying them on other accounts until they gained access.
- **2019 Texas municipalities**—22 municipalities were hit with ransomware attacks, the hackers demanding $2.5 million. Attackers most likely infiltrated through a phishing email, the most common method for such attacks.
- **2019 Quest Diagnostics**—11.9 million records were exposed, including financial and medical information for patients. An unauthorized user accessed an American Medical Collection Agency system which contained the data.

Cyber criminals are focused on obtaining usernames and passwords to access sensitive data.

Hackers are focused on obtaining usernames and passwords, often through phishing emails and credential stuffing. How do you protect your customers and business? By layering multi-factor authentication on top of single sign-on.

Step 1: Reducing the number of passwords with Single Sign-On

According to Verizon's 2019 Data Breach Investigations Report, 29 percent of breaches involved stolen credentials. Passwords are the weak link. Studies show that 72 percent of people have trouble remembering their passwords, which is probably why 70 percent of people reuse them. So chances are, that stolen password can be used somewhere else.

One way companies are addressing the problem is to reduce the number of passwords employees need to access resources. That way, IT can focus on making sure that the single password the user must remember is a secure one. The technology to enable reduced passwords is called single sign-on (SSO).

72 percent of people have trouble remembering their passwords. And 70 percent of people reuse passwords.

Single sign-on enables users to securely sign in to multiple applications and websites by logging in only once—with just one set of credentials (username and password). SSO reduces the number of passwords that employees, contractors, and partners need. Implemented correctly, SSO can give users one password to access all their cloud apps and all their on-prem legacy apps.

How does SSO work?

SSO typically uses the standard protocol called Security Assertion Markup Language (SAML) for authentication with apps. SAML is an XML-based open standard and the product of the OASIS Security Services Technical Committee. Most SaaS vendors already support SAML, making it easy for SSO solutions to work with them. For example, OneLogin's extensive app catalog includes SAML integration of G Suite, Office 365, Workday, Box, Salesforce, and thousands of other apps.

With SAML SSO, applications no longer authenticate the users directly. The apps don't store user passwords, but instead rely on the identity provider (the SSO solution) to perform the authentication and then pass on identity data to the applications. To ensure that only the identity provider can pass the identity data, the two parties rely on digital signatures, which enable the application to verify that the identity data comes from an identity provider it trusts.

If your company is already using Active Directory or LDAP to manage identities, you can simply connect it to OneLogin to keep using AD or LDAP as your system of record. OneLogin is easy to plug into complex directory infrastructures with multiple forests and domains via its Active Directory and LDAP connectors. The connectors ensure that any changes to users and group memberships in the directory are automatically pushed to OneLogin.

OneLogin also integrates with HR solutions such as Workday. If such a solution is your system of record for user identities, OneLogin can provision and de-provision employees and contractors in real-time based on updates to the HR system.

Moving to passwordless authentication

Single sign-on has huge security benefits. When users have trouble remembering passwords, they tend to:

- Use the same password for everything
- Never change their passwords
- Store passwords in plain text

Worst of all, they simply forget the password and request a reset. Over and over again, adding up to lost time and money as your IT staff spends hours and hours just resetting user passwords.

That's why the future is passwordless authentication. SSO gets you most of the way there.

Eliminating passwords literally reduces the number of opportunities for hackers. But, even one stolen password is too many when the password is the only barrier between your corporate data and a criminal.

That's where multi-factor authentication comes in.

WHAT IS SAML?

SAML is an XML-based open standard and the product of the OASIS Security Services Technical Committee.

Step 2: Closing the security gap with multi-factor authentication

Multi-Factor Authentication (MFA) verifies a user's identity by requiring multiple authentication factors instead of relying merely on passwords, which are susceptible to being compromised. Typically, the additional authentication factors are stronger, such as a one-time code that expires within a minute or a biometric factor, such as fingerprint or facial recognition.

Strong authentication factors provide increased assurance about the user's identity since they are not easily compromised. With MFA, a cybercriminal may steal a username and password, but the criminal will be thwarted by having to verify identity in a different manner when attempting to log in.

History of MFA

Authentication has evolved as a technology and continues to do so. We typically talk of three phases in the history of authentication:

PHASE 1

Authentication based on things you **know** (knowledge), such as a password or a PIN.

INCLUDED:

- Usernames
- Passwords

PHASE 2

Authentication based on things you know and things you **have** (possession), such as a badge or smartphone.

INCLUDED:

- Phones
- Smart cards
- Physical devices

PHASE 3

Authentication based on things you know and things you **are** (inheritance), indicated through biometrics, like fingerprints and facial recognition.

INCLUDED:

- Fingerprints
- Eye scanning
- Facial recognition
- Personal security questions

Any additional factor is better than none

Let's face it, any additional factor helps. As the data breaches we discussed at the beginning of this paper show, it's far too easy for cybercriminals to steal usernames and passwords.

But if criminals also have to steal a physical device like a laptop or a phone, the chances of a successful crime go down. It requires a far more coordinated effort to steal a specific user's phone along with their username and password. When you require the user to enter a fingerprint via their smartphone or use facial recognition, you've created another significant impediment to hacking.

That's why more and more companies are looking at adding multi-factor authentication. And it's why cyber insurance companies increasingly require the institutions they insure to use multi-factor authentication.

How OneLogin MFA works

OneLogin MFA provides a streamlined multi-factor authentication solution that increases security without slowing down users. OneLogin MFA includes:

- Simple registration by scanning a QR code with the smartphone
- Push notifications for ease-of-use
- Backup and restore in the event of a lost device
- The ability to verify device hygiene

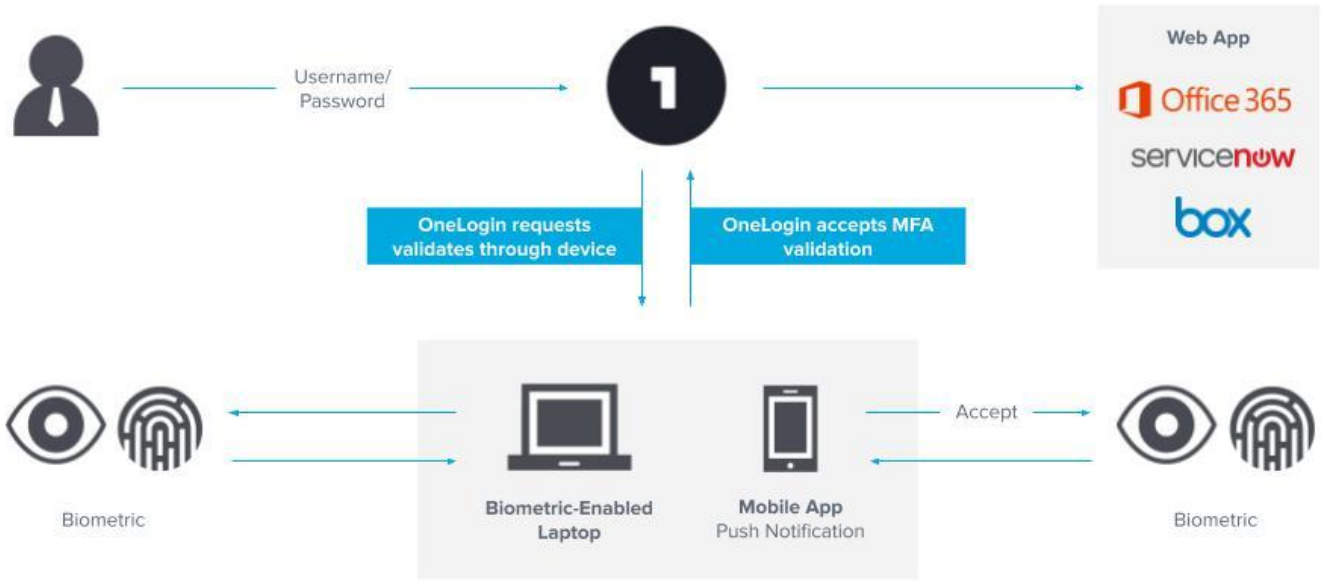
It starts with an easy registration process. Employees can register by simply scanning a QR code with their phone. No typing in a long passcode. No delays as the user enters multiple codes. Users just install OneLogin Protect and scan the QR code.

WHAT IS MFA?

Multi-Factor Authentication (MFA) verifies a user's identity by requiring multiple authentication factors instead of relying merely on passwords.

OneLogin uses push notifications to ensure fast authentication. When an employee or contractor tries to log into an application, OneLogin challenges the user. Let's say the user has a biometric-enabled laptop, OneLogin challenges the user via that device and the user verifies on the laptop with their biometrics.

More commonly, a push notification goes to the user's phone. Instead of users having to open the app on their phone, find a pin, and type it into OneLogin, the user simply presses a button on their device. If required, they also verify on the device with biometrics.



OneLogin MFA supports many different providers and methods, including:

- OneLogin's own mobile app, OneLogin Protect for iOS and Android
- OneLogin OTP for Windows Phones and Windows Desktop
- OneLogin security questions
- One-time code via SMS
- Phone call
- Duo Security
- Google Authenticator
- Symantec VIP Access
- Yubico Yubikey
- RSA SecurID

You can set restrictions on the user's device for added protection, including blocking devices that have been jailbroken and requiring users have a lock screen. And, in the event a device is lost or stolen, users can restore their MFA settings on a new device, if they have used OneLogin's backup and restore feature.

OneLogin multi-factor authentication goes beyond single sign-on to secure user accounts and data. Single sign-on enables users to access everything they need with one password. Multi-factor authentication protects the user against password theft, by requiring an additional piece of data and verifying the identity of the person requesting access.

Step 3: Streamlining the journey with Adaptive Authentication

Nobody wants to slow down work. If you're concerned that adding MFA will complicate or slow the workflow, there are options, because the one thing you can't compromise on is security.

That's where the latest authentication innovation comes in. It's called risk-based or adaptive authentication.

Static rules don't always provide the optimal balance between usability and security. For example, being on the corporate Wi-Fi doesn't necessarily mean that a user login is safe. Conversely, an employee accessing from home via their computer might be perfectly trustworthy if this is the user's normal location and behavior on that device. Adaptive authentication takes user context like this into account.

> "OneLogin has strengthened its adaptive authentication capabilities by incorporating user behavior analytics."
>
> GARRETT BEKKER
>
> 451 Research

OneLogin's Adaptive Authentication uses machine learning to track user behavior across locations and devices in order to build a behavior profile of that user against which authentication decisions can be risk scored in real-time and used to trigger multi-factor authentication. OneLogin determines whether to prompt users for multi-factor authentication (MFA) based on a broad set of inputs, including:

- The user's location and recent travel pattern
- The IP address the user is coming from
- The time of day the user is logging in
- The device the user is accessing from

Risk Factor	Result	Risk Level
Network Reputation		
Flagged in AlienVault Open Threat Exchange	No	Low
Flagged in Project HoneyPot	No	Low
Access from Tor Network	No	Low
New IP address	No	Low
Geographic Location		
New city or country	No	Low
Device Fingerprinting		
New device	Yes	High
New or infrequently used OS	Yes	High
New browser	Yes	High
Time Anomalies		
Unusual time of day	No	Low
Fast user movement	No	Low
Simultaneous access from two distant locations	No	Low

OneLogin Adaptive Authentication scores the risk of each new login attempt based on the profile it has built of the user. Login attempts with elevated risk scores require more authentication.

For different users and groups, you decide whether to default to prompting users for additional factors and only prompt them for less if their risk profile is low. That might be appropriate for those with access to financial data or customer personally identifiable information. Alternatively, you can just ask for a username and password by default and prompt for additional factors when the risk profile indicates a higher risk. With this level of control, you can ensure that each type of user gets the appropriate authentication process and always keep it as streamlined as it is safe.

Conclusion

The heat is on businesses to secure their corporate and customer data. The average cost of a breach in 2018 was $148 per record and $7.91 million in the United States. The impact lasts, too, with companies underperforming on the NASDAQ by -15.58%, three years after a breach. While you have to secure your business, you also have to keep employee authentication fast and easy to maintain productivity.

Single sign-on and MFA are keys to doing so. Single sign-on reduces the number of passwords users need, and therefore for the number of opportunities for hackers. Multi-factor authentication ensures you aren't solely reliant on a password as protection, because it adds other authentication factors. And you can use adaptive authentication, with its machine learning, to prompt users for additional factors only when needed.

The average cost for data breaches is **$148** per record and **$7.91** million per incident in the United States.

About OneLogin

OneLogin, the leader in Unified Access Management, connects people with technology through a simple and secure login, empowering organizations to access the world™. The OneLogin Unified Access Management (UAM) platform is the key to unlocking the apps, devices, and data that drive productivity and facilitate collaboration. OneLogin serves businesses and partners across a multitude of industries, with over 2,500 customers worldwide. We are headquartered in San Francisco, California. For more information, visit www.onelogin.com, blog, Facebook, Twitter or LinkedIn.

Contact us to learn more about OneLogin.

www.onelogin.com/company/contact